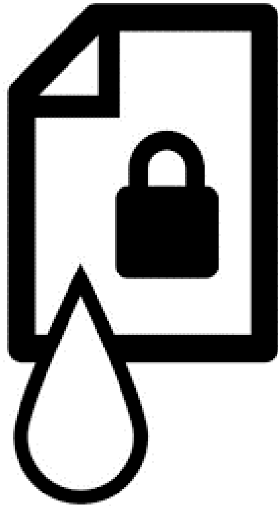
NUTH GEMEENTEBLAD
Officiële uitgave van gemeente Nuth.

Nr. 86838
30 juni
2016

Protocol meldplicht datalekken gemeente Nuth



Gemeente Nuth
Inwerking getreden 1 juli 2016

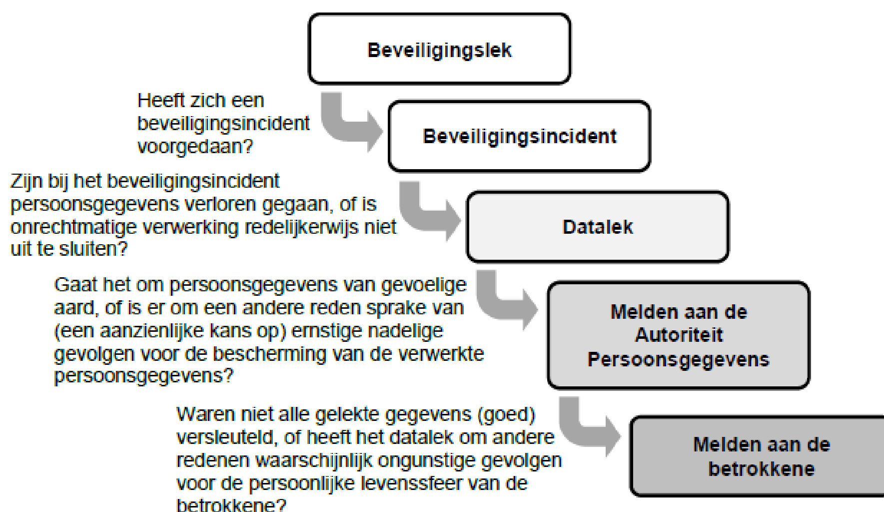
Samenvatting

Op 1 januari 2016 is de meldplicht datalekken als gevolg van een wijziging in de Wet Bescherming Persoonsgegevens in werking getreden. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra een ernstig datalek wordt geconstateerd. Tevens dient men, in een aantal gevallen, het datalek ook te melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Kader
Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Hierin staat dat de persoonsgegevens die wij verwerken beveiligd dienen te worden tegen verlies en tegen onrechtmatige verwerking (artikel 13 Wbp). Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).

Voorliggend protocol maakt deel uit van een groter geheel binnen de organisatie, namelijk het privacyprotocol alsmede het informatiebeveiligingsbeleid. Het privacyprotocol dient ertoe bij te dragen dat er geen datalekken in de organisatie ontstaan. Voorts kan middels het informatiebeveiligheidsbeleid, alsmede de incidentmanagementprocedure, worden nagegaan of er sprake is van een datalek dan wel van een beveiligingsincident.

Afwegingen
Bij de beslissing of een gebeurtenis die zich heeft voorgedaan gemeld moet worden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, dient een aantal afwegingen gemaakt te worden. Het onderstaande schema geeft deze afwegingen weer.



Datalek
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet bijvoorbeeld gedacht worden aan het kwijtraken van een USB-stick, diefstal van een laptop of een inbraak door een hacker.

Echter, niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet uitgesloten kan worden. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens. Indien er sprake is van een beveiligingsincident dient, ongeacht of er sprake is van een datalek, de incidentmanagementprocedure te worden gevolgd.

Melden aan de Autoriteit Persoonsgegevens
Niet ieder datalek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. Volgens de wet dient slechts melding aan de Autoriteit Persoonsgegevens gedaan te worden, als het datalek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard kan gedacht worden aan:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits-)fraude*
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat een datalek gemeld moet worden waarbij persoonsgegevens van slechts één persoon betrokken zijn.

Een melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan **72 uur** na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar gesteld (raadpleegbaar via: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0). Via dit webformulier kan de melding indien nodig aangevuld of ingetrokken worden

Melden aan de betrokkene
Als geconcludeerd wordt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dat niet automatisch dat dit datalek ook gemeld dient te worden aan de betrokkene. Hiervoor dient een aparte afweging gemaakt te worden.

De wet geeft aan dat een melding gedaan moet worden aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij kan gedacht worden aan bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kan er in principe van uit gegaan worden dat het datalek niet alleen gemeld moet worden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door bijvoorbeeld een gelekt wachtwoord te vervangen. De wet schrijft voor dat de melding onverwijld gedaan moet worden. Hierbij moet rekening worden gehouden met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd wordt, hoe eerder hij/zij in actie kan komen.

Als passende technische beschermingsmaatregelen zijn genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven. Per geval dient bepaald te worden of de maatregelen die zijn getroffen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

Boete
Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro.

Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bijvoorbeeld bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

Inleiding

Met ingang van 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens (Wbp) in werking getreden die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens en - in bepaalde situaties - ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt. Bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt moeten zelf een afweging maken of een concreet datalek, dat hen ter kennis komt, onder het bereik van de wettelijke meldplicht valt.

Dit protocol is gebaseerd op de beleidsregels van de Autoriteit Persoonsgegevens, welke dienen als uitgangspunt bij het toepassen van handhavende maatregelen inzake de meldplicht datalekken. Deze beleidsregels gaan in op de meldplicht datalekken die is opgenomen in de Wbp. De beleidsregels van de Autoriteit Persoonsgegevens zijn in werking getreden met ingang van 1 januari 2016, zijnde de datum van inwerkingtreding van de meldplicht datalekken. In de loop van 2017 zullen de beleidsregels worden geëvalueerd en waar nodig aangepast. Inherent voortvloeisel hieruit is dat onderhavig protocol van de gemeente Nuth eind 2017 zal worden geëvalueerd en zo nodig herzien.

Verdere informatie over de beveiliging van persoonsgegevens en over de meldplicht datalekken is te vinden op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Leeswijzer
In het eerste hoofdstuk worden ingegaan op de uitleg van enkele belangrijke begrippen welke van betekenis zijn in voorliggend protocol. Voorts wordt in het tweede hoofdstuk, middels een schema en de beantwoording van een drietal vragen, nagegaan of de meldplicht datalekken al dan niet van toepassing is op de gemeente Nuth. In hoofdstuk drie wordt vervolgens ingegaan op het verwerken van persoonsgegevens door bewerkers. Hierbij wordt met name aandacht besteed aan het opstellen van afspraken met bewerkers in de vorm van bewerkersovereenkomsten. Het vierde hoofdstuk geeft voorts een stappenplan weer dat gevolgd kan worden om na te gaan of er sprake is van een datalek en of dit datalek al dan niet gemeld dient te worden aan de Autoriteit dan wel de betrokkene(n). In hoofdstuk vijf wordt kort weergegeven welke gegevens geïnventariseerd dienen te worden indien een datalek zich voordoet. In het zesde en tevens laatste hoofdstuk van dit protocol wordt ingegaan op het register van datalekken, alsmede eventuele handhavingsmogelijkheden welke ingezet kunnen worden door de Autoriteit Persoonsgegevens.

1. Definities

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare persoon (artikel 1, sub a, Wbp). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Bestand
Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (artikel 1, sub c, Wbp).

Verantwoordelijke
Degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking. De bevoegdheden kunnen soms in verschillende handen liggen, er is dan sprake van gezamenlijke verantwoordelijkheid.

Bewerker / Verwerker
Deze verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen (artikel 1, sub e, Wbp). Als bewerker kunnen worden aangemerkt ketenpartners (zoals Wijzelf of Kompas) die persoonsgegevens verwerken of derde partijen zoals IT-leveranciers die zorg dragen voor het onderhoud en beheer van systemen en/of applicaties en/of gegevensbestanden waar persoonsgegevens onderdeel van uit maken of bij betrokken worden, zoals PinkRoccade voor het Burgerzakensysteem, Gemeente Beek voor de Gegevensmakelaar, Parkstad IT voor de serversystemen van de gemeente Nuth en Infosupport voor het regiesysteem voor het sociaal domein. Een verwerker staat gelijk aan bewerker.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft (artikel 1, sub f, Wbp).

Derde
Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken (artikel 1, sub g, Wbp).

Ontvanger
Degene aan wie de persoonsgegevens worden verstrekt (artikel 1, sub h, Wbp).

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, beheren, onderhouden, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

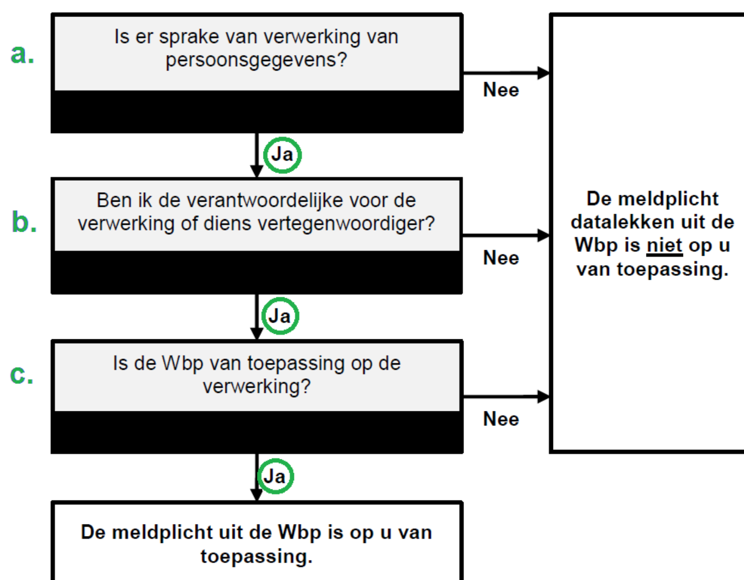
Verstrekking van persoonsgegevens

Het bekendmaken of ter beschikking stellen van persoonsgegevens (artikel 1, sub n, Wbp).

Verzamelen van persoonsgegevens
Het verkrijgen van persoonsgegevens (artikel 1, sub o, Wbp).

2. Is de meldplicht datalekken van toepassing?

Onderstaand schema geeft enkele vragen weer die beantwoord dienen te worden om vast te stellen of de meldplicht datalekken uit de Wbp van toepassing is. Middels groene cirkels zijn de vragen vanuit het oogpunt van de gemeente Nuth beantwoord.



<u>Toelichting:</u>

a. ***Is er sprake van verwerking van persoonsgegevens?***
Ja, er is binnen de gemeente Nuth sprake van verwerking van persoonsgegevens. Verwerking van persoonsgegevens betreft namelijk elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

b. ***Ben ik de verantwoordelijke voor de verwerking of diens vertegenwoordiger?***
Ja, de gemeente Nuth is verantwoordelijk voor de verwerking. De verantwoordelijke is namelijk degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Een verantwoordelijke kan een vertegenwoordiger aanwijzen die namens hem de verplichtingen uit de Wbp nakomt.

c. ***Is de Wbp van toepassing op de verwerking?***
Ja, de Wbp is van toepassing op de verwerking. Hierbij zijn twee elementen van belang, namelijk de aard en de doelstelling van de verwerking. Bepaalde verwerking vallen door hun aard of doelstelling buiten de reikwijdte van de Wbp en op deze verwerkingen is de meldplicht datalekken niet van toepassing. Ten tweede is het van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt.

Voorts blijkt ingevolge artikel 1 sub d van de Wet bescherming persoonsgegevens dat de Wbp van toepassing is op overheidsinstellingen.

3. Verwerking van persoonsgegevens door bewerker(s)

Verwerking van persoonsgegevens door bewerker(s) omvat onder andere:

- Persoonsgegevens die t.b.v. de gemeentelijke dienstverlening door ketenpartijen zoals Wijzelf of Kompas worden verwerkt ;
- IT-leveranciers die een systeem of toepassing waarin persoonsgegevens worden verwerkt als cloudoplossing aanbieden, zoals Infosupport met het regiesysteem c2Go voor WMO en Jeugdzorg of PinkRoccade met het Burgerzakensysteem iBurgerzaken;
- IT-leveranciers die een systeem of toepassing beheren of onderhouden t.b.v. de gemeente Nuth zoals Parkstad IT of de gemeente.

Waarborgen

Bij verwerking door een bewerker dient de gemeente te zorgen voor voldoende waarborgen en toe te zien op de naleving (artikel 14, eerste en derde lid, Wbp):

"Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen. De verantwoordelijke draagt zorg dat de bewerker:

a. *de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid, Wbp; en*

b. *de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13 Wbp; en*

c. *de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplich- ting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, die leidt tot aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt."*

De gemeente bewaakt als verantwoordelijke dat er samenwerkingsafspraken worden vastgelegd met deze bewerkers (partners) waarin een zorgvuldige en rechtmatige gegevensverwerking wordt geborgd.

Waarover moeten afspraken gemaakt worden met de bewerker?

De wet schrijft niet specifiek voor wat met een bewerker afgesproken dient te worden. Er kan echter gedacht worden aan de navolgende aspecten: Gaat de bewerker de gemeente daadwerkelijk informeren over alle relevante incidenten en zo ja, hoe? Gaat de bewerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens? Ontvangt de gemeente per incident alle informatie die nodig is? Wordt de gemeente tijdig geïnformeerd over de incidenten? Wordt de gemeente op de hoogte gehouden van eventuele nieuwe ontwikkelingen m.b.t. het incident en van de maatregelen die de bewerker treft om de gevolgen te beperken en herhaling te voorkomen?

Hoe moeten afspraken met de bewerker(s) worden gemaakt?

De afspraken tussen de gemeente en de bewerker(s) dienen schriftelijk vastgelegd te worden ingevolge artikel 14, tweede en vijfde lid, Wbp, in een bewerkersovereenkomst.

"De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 Wbp schriftelijk of in een andere, gelijkwaardige vorm vastgelegd."

Opbouw bewerkersovereenkomst

Beveiligingsmaatregelen die de bewerker moet treffen om aan de betrouwbaarheidseisen te voldoen alsmede de wijze waarop de gemeente toeziet op de naleving, worden vastgelegd in een bewerkersovereenkomst.

Een bewerkersovereenkomst dient onder andere het navolgende duidelijk weer te geven:

" De gemeente Nuth draagt zorg dat [de bewerker] voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen."

"De gemeente Nuth draagt zorg dat [de bewerker] de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13."

"De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke."

"Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd."

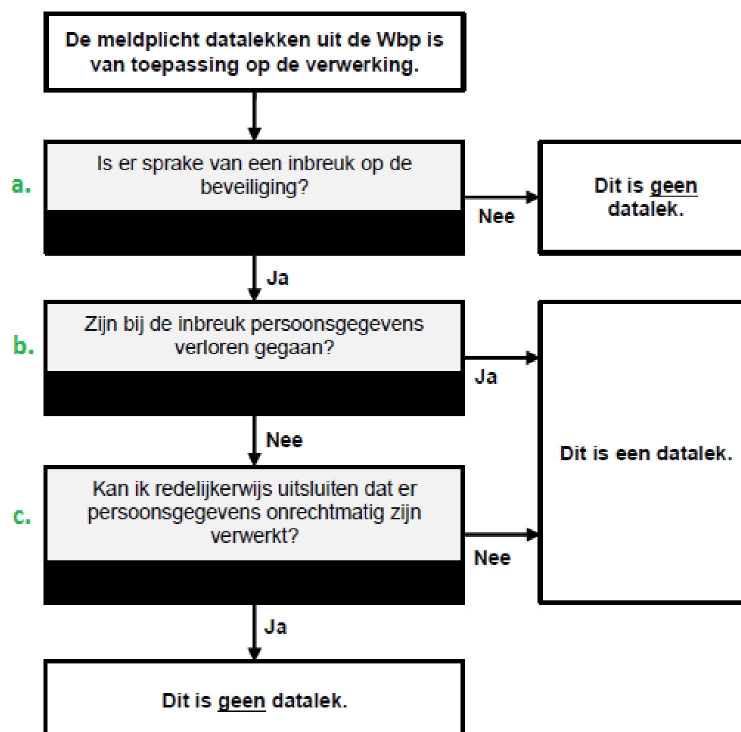
Waar let de Autoriteit Persoonsgegevens op in het kader van bewerkersovereenkomsten?
Bij de beoordeling van de afspraken in bewerkersovereenkomsten besteedt de Autoriteit Persoonsgegevens in ieder geval aandacht aan de navolgende onderwerpen:

- *Dienstverlening door de bewerker:* een omschrijving van de dienst(en) die de bewerker verleent en de persoonsgegevens die de bewerker daarbij verwerkt. Verder wordt omschreven welke (groepen) medewerkers van de bewerker toegang hebben tot welke persoonsgegevens en welke handelingen deze medewerkers mogen uitvoeren met de persoonsgegevens. Denk hierbij aan consultants, en IT personeel zoals Helpdesk medewerkers, systeembeheerders en ontwikkelaars. Er is een expliciet verbod opgenomen om andere handelingen met de persoonsgegevens uit te voeren dan wat hier is omschreven.
- *De betrouwbaarheidseisen die op de verwerking van toepassing zijn:* deze dienen gedifferentieerd te zijn op basis van de gevoeligheid van de verwerkte persoonsgegevens.
- *De beveiliging door de bewerker:* afspraken over de technische en organisatorische beveiligingsmaatregelen waarmee de bewerker invulling geeft aan de betrouwbaarheidseisen.
- *Transparantie over de beveiliging:* afspraken over de inhoud en frequentie van rapportages die de bewerker aan de gemeente oplevert over de beveiliging. Hierin dient een omschrijving te worden opgenomen van het recht van de gemeente om de naleving van de beveiligingsmaatregelen door onafhankelijke deskundigen vast te laten stellen (bijv. IT-auditors).
- *Transparantie over opgetreden beveiligingsincidenten:* afspraken over de inhoud van rapportages over beveiligingsincidenten en datalekken, de criteria voor rapportage van incidenten en de snelheid waarmee wordt gerapporteerd. In de afspraken dient te worden opgenomen dat de bewerker beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen meteen rapporteert en dat de bewerker waar nodig ook meewerkt aan het adequaat informeren van betrokkenen.
- *Verwerking door subbewerkers:* afspraken over het al dan niet toestaan van verwerking door subbewerkers, met daarbij de eventuele beperkingen (bijv. dat de subbewerkers geen subbewerkers mogen inschakelen). Als bewerking door subbewerkers is toegestaan, dan is in de bewerkersovereenkomst opgenomen dat met de subbewerkers overeenkomsten moeten worden afgesloten en dat alle verplichtingen uit de bewerkersovereenkomst die relevant zijn voor de beveiliging van de verwerkte persoonsgegevens daarin moeten worden overgenomen.
- *Verwerking van persoonsgegevens buiten Nederland:* afspraken over welke persoonsgegevens in welke landen worden verwerkt.
- *Voorwaarden voor heronderhandeling of beëindiging van de overeenkomst:* Afspraken over heronderhandeling van de bewerkersovereenkomst als een wijziging in de verwerkte persoonsgegevens of in de betrouwbaarheidseisen daar aanleiding toe geeft. Bij de afspraken is ook een noodplan opgenomen voor het geval een van de partijen de relatie wil beëindigen voor het einde van de looptijd van de overeenkomst. Verder is vastgelegd hoe en in welke vorm de verantwoordelijke de verwerkte persoonsgegevens weer ter beschikking krijgt en hoe wordt geborgd dat de bewerker na het beëindigen van de relatie niet meer over de persoonsgegevens kan beschikken.

De verantwoordelijke stelt vast dat de afspraken in de bewerkersovereenkomst daadwerkelijk worden nageleefd ingevolge artikel 14, eerste lid, Wbp:
"De verantwoordelijke ziet toe op de naleving van [de technische en organisatorische beveiligingsmaatregelen door de bewerker]."

4. Stappenplan constatering (en melding) datalek

4.1 Nagaan of er sprake is van een datalek



Toelichting:

a. ***Is er sprake van een inbreuk op de beveiliging?***
Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan en eventueel getroffen preventieve maatregelen waren niet toereikend om dit te voorkomen.
- **Voorbeelden**: een kwijtgeraakte USB-stick; een gestolen laptop; een inbraak door een hacker; een calamiteit zoals een brand in een datacentrum etc.
- **Kenmerken**: het beveiligingsincident heeft daadwerkelijk gevolgen voor de persoonsgegevens die worden verwerkt. Er zijn persoonsgegevens verloren gegaan of er kan niet redelijkerwijs uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt. De repressieve maatregelen en de herstelmaatregelen die eventueel zijn getroffen waren niet voldoende om de gevolgen geheel weg te nemen.

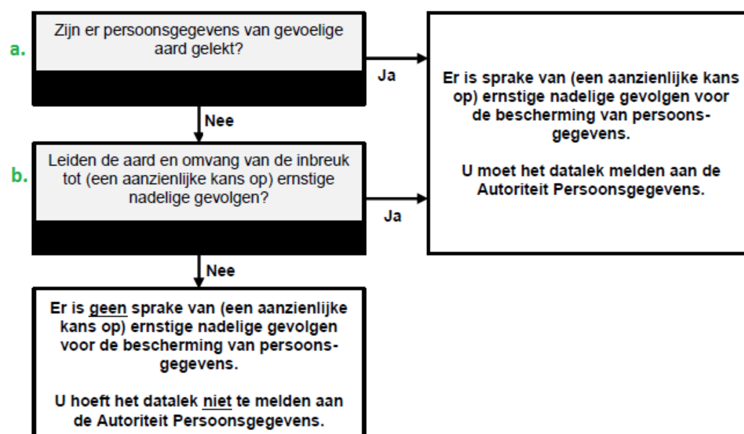
b. ***Zijn bij de inbreuk persoonsgegevens verloren gegaan?***
Er is sprake van een datalek als de persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en er geen actuele reservekopie beschikbaar is.

c. ***Kan redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt?***
Als redelijkerwijs niet uitgesloten kan worden dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet de inbreuk beschouwd worden als een datalek.

4.2 Nagaan of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat een inbreuk alleen gemeld hoeft te worden als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp).

Het is aan de gemeente om te bepalen of een datalek dat is ontdekt binnen de reikwijdte van de meldplicht datalekken aan de Autoriteit Persoonsgegevens valt. Deze afweging kan middels onderstaande vragen ondersteund worden:



Toelichting:

a. ***Zijn er persoonsgegevens van gevoelige aard gelekt?***

Hierbij moet gekeken worden naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij persoonsgegevens van gevoelige aard kunnen verlies of onrechtmatige verwerking o.a. leiden tot stigmatisering of uitsluiting van de betrokkene, tot financiële schade of (identiteits)fraude. Tot deze categorie van persoonsgegevens moet in ieder geval worden gerekend:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp: bijvoorbeeld over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid.
- Gegevens over de financiële situatie van betrokkene: bijvoorbeeld gegevens over schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene: bijvoorbeeld gegevens over een gokverslaving, prestaties op school of werk.
- Gebruikersnamen, wachtwoorden en andere inloggegevens.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude: bijvoorbeeld kopieën van identiteitsbewijzen en burgerservicenummer (bsn).

b. ***Leiden aard en omvang van de inbreuk tot (aanzienlijke kans op) ernstige nadelige gevolgen?***

De aard en omvang van de getroffen verwerking moet mede bepalend zijn voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens. Beveiligingslekken in de omvangrijke verwerking van persoonsgegevens waarover de gemeente Nuth beschikt kunnen ook zeer grote gevolgen hebben voor betrokkenen.

Behalve voor aard en omvang van de getroffen verwerking wordt ook aandacht gevraagd voor de positie van kwetsbare groepen (bijvoorbeeld mensen die te maken hebben met stalking of in een blijf-van-mijn-lijfhuis verblijven). Voor deze groepen kan verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen.

Voorbeelden :

Enkele voorbeelden van datalekken welke moeten worden gemeld aan de Autoriteit Persoonsgegevens:

- *Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens;*
- *Een medewerker verliest een USB of laptop met onversleutelde gegevens van burgers;*
- *Door een beveiligingslek blijkt dat persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen) van werknemers door onbevoegden zijn ingezien;*
- *Enkele personeelsleden maken gebruik van het wachtwoord van een ander persoon om toegang te krijgen tot persoonsgegevens. Er is op onrechtmatig wijze toegang verkregen tot persoonsgegevens. Bovendien is er sprake van een schending van interne voorschriften. Disciplinaire maatregelen liggen voorts voor de hand.*

Enkele voorbeelden van gebeurtenissen die niet onder de meldplicht vallen:

- *Een brief met daarin persoonsgegevens wordt naar een fout adres gestuurd, maar wordt ongeopend retour gezonden;*

- *Iemand laat een koffer met daarin persoonsgegevens achter in de trein, maar dit is voorzien van een deugdelijk slot en komt vervolgens ongeopend retour bij de eigenaar;*

4.3 Wanneer en hoe dient het datalek gemeld te worden aan de Autoriteit Persoonsgegevens?

Het datalek moet onverwijld gemeld worden aan de Autoriteit Persoonsgegevens (artikel 34a, eerste lid, Wbp). Het onverwijld melden houdt in dat, na het ontdekken van een mogelijk datalek, enige tijd genomen mag worden voor nader onderzoek teneinde een onnodige melding te voorkomen.

De termijn voor het melden van het datalek begint te lopen op het moment dat de gemeente zelf, of een bewerker die de gemeente heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt.

Zonder onnodige vertraging, en zo mogelijk binnen **72 uur** na de ontdekking, dient melding te worden gedaan bij de Autoriteit Persoonsgegevens, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien het incident later dan 72 uur na ontdekking aan de toezichthouder wordt gemeld, dan kan desgevraagd gemotiveerd worden waarom de melding later is gedaan. Het is mogelijk dat na 72 uur na de ontdekking van het incident nog niet volledig inzichtelijk is wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt de melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog aangevuld of ingetrokken worden.

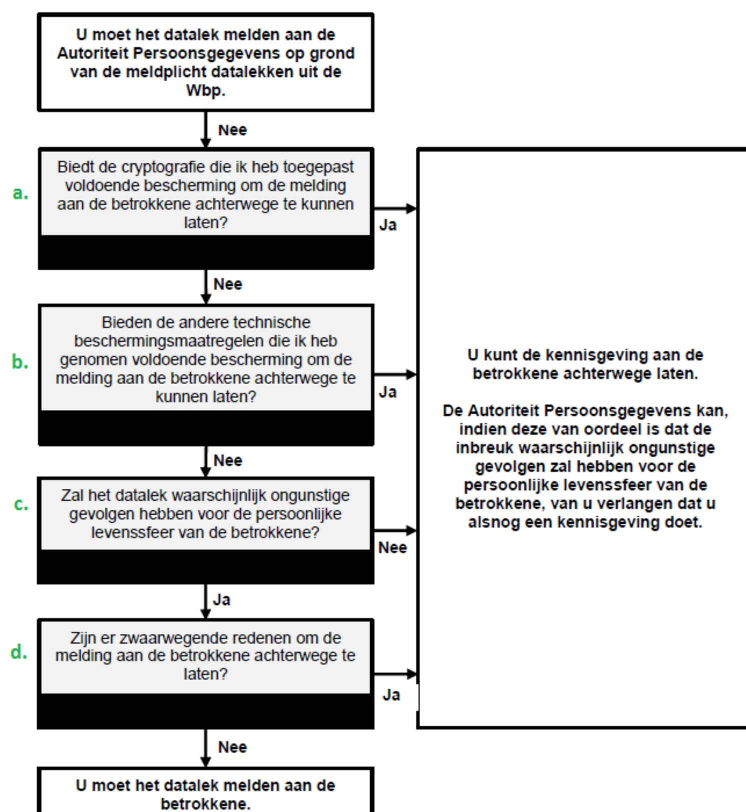
Om datalekken tijdig te kunnen melden zullen ook goede afspraken gemaakt moeten worden met de bewerkers, zodat ook tijdig en adequaat informatie verstrekken over alle relevante incidenten.

De Autoriteit Persoonsgegevens heeft een webformulier beschikbaar gesteld waarmee datalekken kunnen worden gemeld. Dit webformulier is raadpleegbaar middels onderstaande link:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
Tevens kunnen de gevraagde gegevens per fax toegezonden worden aan de Autoriteit Persoonsgegevens. Hierbij moet wel aangetoond kunnen worden dat de melding tijd is gedaan.

Vervolgens verstuurd de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie zal contact worden opgenomen om de herkomst van de melding te verifiëren.

4.4 Dient het datalek gemeld te worden aan de betrokkene?

4.4.1 Stappenplan melden aan betrokkenen ja/nee:



<u>Toelichting:</u>

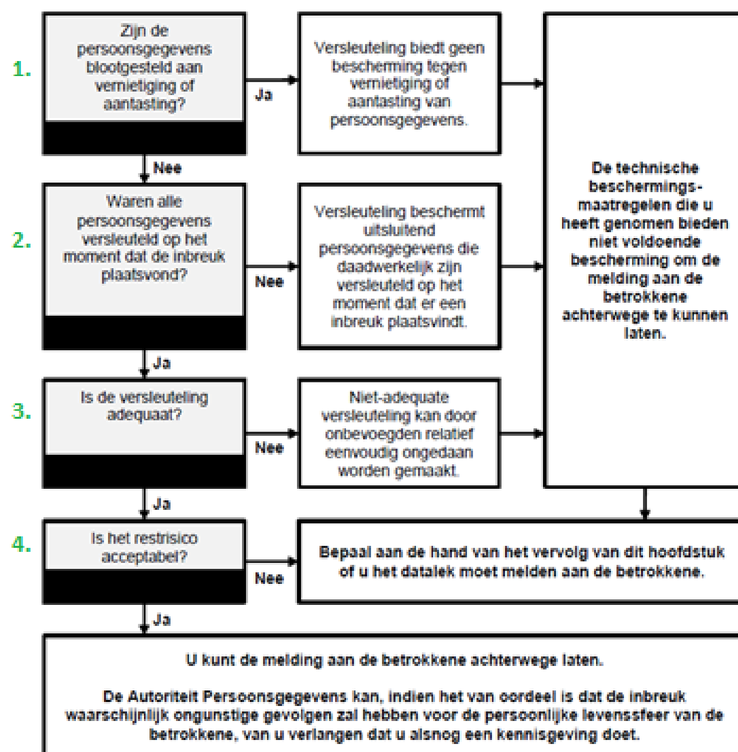
a. ***Biedt de cryptografie die is toegepast voldoende bescherming om melding aan de betrokkene achterwege te kunnen laten?***

Indien passende technische beschermingsmaatregelen zijn genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan betrokkene achterwege blijven (artikel 34a, zes lid, Wbp).

Er zijn twee soorten cryptografische bewerkingen:

- Encryptie = versleuteling. Deze bewerking is omkeerbaar aangezien door gebruik van de juiste sleutel de oorspronkelijke informatie kan worden verkregen (decryptie)
- Hashing = het omzetten van gegevens in een unieke code. Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden.

Onderstaand wordt een aanvullend schema weergegeven ter beoordeling of de technische beschermingsmaatregelen die genomen zijn voldoende bescherming hebben geboden om melding aan de betrokkene achterwege te kunnen laten:



1. *Zijn persoonsgegevens blootgesteld aan vernietiging of aantasting?*
   Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem/haar worden gemeld.
2. *Waren de persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?*
   Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.
3. *Is de versleuteling adequaat?*
   Bij gebruik van cryptografische bewerkingen dient periodiek beoordeeld te worden of deze nog voldoende bescherming bieden.
4. *Is het restrisico acceptabel?*
   Per concreet geval zal beoordeeld moeten worden of de geboden bescherming voldoende is om de kennisgeving aan betrokkene achterwege te kunnen laten. Hierbij moet ook meegewogen worden welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

b. ***Bieden de andere technische beschermingsmaatregelen die zijn toegepast voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?***
Onder deze technische beschermingsmaatregelen kan worden verstaan: “remote wiping” en “pseudonimisering”. Middels “remote wiping” worden persoonsgegevens beschermd tegen onbevoegde kennisname. Bij deze methode wordt gegevens die op een apparaat staan op afstand gewist en daardoor ontoegankelijk voor onbevoegden. “Pseudonimisering” betekent dat technische maatregelen worden genomen om te voorkomen dat persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene. Het zorgt ervoor dat persoonsgegevens onbegrijpelijk worden gemaakt voor onbevoegden en de kans dat een datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkene als gevolg daarvan wordt verlaagd.

c. ***Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene?***
Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp). Betrokkenen

kunnen door het verlies, onrechtmatig gebruik of misbruik van hun persoonsgegevens namelijk in hun belangen worden geschaad. De schade kan van materiële of immateriële aard zijn. Onder immateriële schade kan worden verstaan: aantasting in eer en goede naam of identiteitsfraude.

Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet ervan uitgegaan worden dat het datalek niet alleen gemeld moet worden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Door deze kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij/zij zich – voor zover dat mogelijk is – daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen.

d. ***Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?***
De melding aan betrokkene mag achterwege blijven als daarvoor zwaarwegende redenen aanwezig zijn. Hierbij geldt wel dat de melding aan de betrokkene alléén achtewege mag blijven als dit noodzakelijk is met het oog op de belangen zoals genoemd in artikel 43 Wbp.

4.4.2 Wanneer moet het datalek gemeld worden aan de betrokkene?
Indien is gebleken dat het datalek aan betrokkene gemeld dient te worden, dient dit onverwijld te geschieden (artikel 34a, tweede lid, Wbp). Dit houdt in dat, na het ontdekken van het datalek, nog enige tijd genomen mag worden voor nader onderzoek. Dit zorgt ervoor dat de betrokkene op een behoorlijke en zorgvuldige manier geïnformeerd kan worden. Hierbij moet wel rekening worden gehouden met het feit dat de betrokkene mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene wordt geïnformeerd, hoe eerder deze in actie kan komen.

In de melding aan de Autoriteit Persoonsgegevens moet aangeven worden of het datalek al aan de betrokkene is gemeld en, wanneer dit niet het geval is, wanneer dit alsnog gedaan zal worden. De termijn die in de melding aan de Autoriteit Persoonsgegevens wordt aangegeven, moet ook worden nagekomen.

4.4.3 Hoe dient het datalek gemeld te worden aan de betrokkene?
Bij de kennisgeving aan de betrokkene dient in ieder geval vermeld te worden:
- Aard van de inbreuk;
- Instanties waar de betrokkene meer informatie over de inbreuk kan krijgen;
- Eventueel te treffen maatregelen die de betrokkene wordt aanbevolen om negatieve gevolgen van de inbreuk te beperken (artikel 34a, derde lid, Wbp).

Bij het beschrijven van de aard van de inbreuk kan doorgaans volstaan worden met een algemene omschrijving. Voorts wordt hierbij de contactgegevens opgenomen zodat de betrokkene terecht kan indien hij/zij vragen heeft over het datalek. Verder kan aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken.

Het belangrijkste is dat zoveel mogelijk betrokkenen bereikt worden met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zoveel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaalgesproken niet bereikt.

5. Welke gegevens moeten worden vastgelegd?

Er dient uitsluitend een overzicht te worden bijgehouden van alle datalekken die onder de meldplicht vallen. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen (artikel 34a, achtste lid, Wbp).

Daar de wet niet voorschrijft hoelang het overzicht bewaart moet worden, mag worden uitgegaan van een bewaartermijn van minimaal een jaar. Indien technische beschermingsmaatregelen voldoende bescherming hebben geboden om de melding aan de betrokkene achterwege te kunnen laten, of als er zwaarwegende redenen zijn geweest om de melding aan betrokkene achterwege te laten, dan dient het overzicht minimaal drie jaar te worden bewaard. Hierbij dient periodiek geëvalueerd te worden of het datalek alsnog aan de betrokkene gemeld moet worden.

Gegevens worden bewaard voor de volgende doeleinden:
- Lering trekken uit het datalek en de wijze waarop is gehandeld;
- Antwoord kunnen geven op vragen van betrokkenen en anderen;

- Alsnog melden van het datalek aan betrokkenen indien dit in eerste instantie achterwege is gelaten en de omstandigheden vereisen dat dit alsnog wordt gedaan.

Verder dient rekening te worden gehouden met het feit dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat indien dit aan de orde is, bewijsmateriaal verzameld moet worden.

6. Wat doet de Autoriteit Persoonsgegevens met de melding?

Na het melden van een datalek stuurt de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging. Als de melding de Autoriteit Persoonsgegevens aanleiding geeft tot nadere actie, dan zal deze daarover contact opnemen.

Het is de eigen verantwoordelijkheid om de oorzaak van het datalek op te sporen en om maatregelen te treffen om herhaling te voorkomen. Het is ook de eigen keuze om de betrokkene al dan niet te informeren.

De ontvangen datalekmeldingen stellen de Autoriteit Persoonsgegevens in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijk raken of waarvan zij last kunnen ondervinden. Als het datalek niet is gemeld aan de betrokkene en deze waarschijnlijk ongunstige gevolgen zal hebben voor de betrokkene, kan de Autoriteit verlangen dat alsnog een kennisgeving wordt gestuurd (artikel 34a, zevende lid, Wbp). Dit staat gelijk aan een bindende aanwijzing. Het niet nakomen kan voorts worden bestraft met een bestuurlijke boete.

6.1 Register van ontvangen datalekmeldingen

De Autoriteit Persoonsgegevens houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. De Autoriteit kan op basis van de gedane meldingen in jaarverslagen of andere publicaties op geanonimiseerd niveau aandacht besteden aan datalekken.

De Autoriteit houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en kan derhalve onderzoek doen naar de mogelijke overtredingen van de wet (artikel 60 Wbp). Hiervoor kan de Autoriteit gebruik maken van informatie uit de ontvangen datalekmeldingen.

6.2 Handhaving

Bij overtreding van datgene dat bij of krachtens artikel 34a Wbp wordt bepaald, kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Als sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de toezichthouder direct een bestuurlijke boete opleggen (artikel 66, vierde lid, Wbp). Indien er geen sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, gaat een bindende aanwijzing vooraf aan het opleggen van een bestuurlijke boete. De Autoriteit kan de overtreder dan een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd (artikel 66, derde lid, Wbp). Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval.

Nuth, 14 juni 2016

Burgemeester en Wethouders vanm Nuth,
De seceretaris,
Drs. H.M.J. van Mierlo
de burgemeester,
D.H. Schmalschláger,

Bijlage I: gegevens in de melding

Deze bijlage bevat gegevens die opgegeven moeten worden als een datalek wordt gemeld aan de Autoriteit Persoonsggevens.

Aard van de melding

1) Is dit een vervolg op een eerdere melding?
   a) Ja (ga verder naar vraag 2)
   b) Nee (ga verder naar vraag 5)

2) Wat is het nummer van de oorspronkelijke melding

3) Wat is de strekking van de vervolgmelding?
   a) Toevoegen of wijzigen van informatie betreffende de eerdere melding (ga verder naar vraag 5)
   b) Intrekking van de eerdere melding (ga verder naar vraag 4)

4) Wat is de reden van intrekking?

Wettelijk kader voor de melding

5) Op grond van welke wettelijke bepaling doet u deze melding?
   a) Artikel 34a, eerste lid, van de Wbp
   b) Artikel 11.3a, eerste lid, van de Tw

Algemene informatie en contactgegevens

6) Over welk bedrijf of welke organisatie gaat het? (vul onderstaande gegevens in)
   a) Naam van het bedrijf of de organisatie: ______________
   b) (bezoek)Adres: __________________________________
   c) Postcode: ______________________________________
   d) Plaats: ____
   e) KvK-nummer: ___________________________________

7) Door wie wordt het datalek gemeld? (vul onderstaande gegevens in)
   a) Naam van de persoon die meldt: ___________________
   b) Functie van de persoon die meldt: _________________
   c) E-mailadres van de persoon die meldt: ______________
   d) Telefoonnummer van de persoon die meldt: __________
   e) Alternatief telefoonnummer: ______________________

8) Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding? (vul onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek)
   a) Naam contactpersoon:___________________________
   b) Functie van de contactpersoon: ___________________
   c) E-mailadres contactpersoon: ______________________
   d) Telefoonnummer contactpersoon: _________________
   e) Alternatief telefoonnummer: ______________________

9) In welke sector is het bedrijf of de organisatie actief?
   ____

Gegevens over het datalek

10) Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

11) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (vul de aantallen in)

a) Minimaal: ____
b Maximaal: ____

12) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

13) Wanneer vond de inbreuk plaats? (kies een van de volgende opties en vul waar nodig aan)
a) Op (datum) __________
b) Tussen (begindatum periode) _______ en (einddatum periode) ________
c) Nog niet bekend

14) Wat is de aard van de inbreuk? (er kunnen meerdere mogelijkheden worden aangekruist)
a) Lezen (vertrouwelijkheid)
b) Kopiëren
c) Veranderen (integriteit)
d) Verwijderen of vernietigen (beschikbaarheid)
e) Diefstal
f) Nog niet bekend

15) Om welk type persoonsgegevens gaat het? (er kunnen meerdere mogelijkheden worden aangekruist)
a) Naam-, adres- en woonplaatsgegevens
b) Telefoonnummers
c) E-mailadressen of andere adressen voor elektronische communicatie
d) Toegangs- of identificatiegegevens
e) Financiele gegevens
f) Burgerservicenummer of sofinummer
g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
h) Geslacht, geboortedatum en/of leeftijd
i) Bijzondere persoonsgegevens (bijv. ras, etniciteit, criminele gegevens, politieke overtuiging etc.)
j) Overige gegevens, namelijk (aanvullen)

16) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (er kunnen meerdere mogelijkheden worden aangekruist)
a) Stigmatisering of uitsluiting
b) Schade aan de gezondheid
c) Blootstelling aan (identiteits)fraude
d) Blootstelling aan spam of phishing
e) Anders, namelijk (aanvullen)

Vervolgacties naar aanleiding van het datalek
17) Welke technische en organisatorische maatregelen heeft de organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Inlichting van de betrokkenen
18) Is het datalek gemeld aan de betrokkenen of wordt het datalek nog gemeld aan de betrokkenen? (kies een van de volgende opties)
a) Ja (ga verder naar vraag 19)
b) Nee (ga verder naar vraag 23)
c) Nog niet bekend

19) Wanneer is het datalek gemeld aan de betrokkenen of wanneer wordt het datalek gemeld?
a) Het datalek is aan de betrokkenen gemeld op (datum) __________

b) Het datalek wordt aan betrokkenen gemeld op (datum) _________
c) Nog niet bekend

20) Wat is de inhoud van de melding aan de betrokkenen? (letterlijke weergave)

21) Hoe veel betrokkenen zijn in kennis gesteld of worden in kennis gesteld?

22) Welk(e) communicatiemiddel(en) zijn/worden gebruik bij het in kennis stellen van de betrokkenen?

23) Waarom wordt afgezien van het melden van het datalek aan de betrokkenen?
a) De technische beschermingsmaatregelen die zijn getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
b) Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (aanvullen)
c) Er zijn zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (aanvullen)
d) Anders, namelijk: (aanvullen)

Technische beschermingsmaatregelen

24) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk/ontoegankelijk gemaakt voor onbevoegden? (vul waar nodig aan)
a) Ja (ga verder naar vraag 25)
b) Nee (ga verder naar vraag 26)
c) Deels, namelijk ___________ (ga verder naar vraag 25)

25) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?

Internationale aspecten

26) Heeft de inbreuk betrekking op personen in andere EU-landen?
a) Ja
b) Nee
c) Nog niet bekend

27) Is het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
a) Ja, namelijk ____________
b) Nee

Vervolgmelding

28) Is de melding compleet?
a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk